IN THE CLAIMS

We claim

1. A method for facilitating content downloads via an insecure communications channel, comprising:

receiving from a device via an insecure communications channel at least one shared secret in encoded form that functions as an identifier of the device;

transmitting encrypted content via the insecure communications channel from a content server to the device;

receiving the shared secret in plaintext form via a secure communications channel;

receiving a confirmation authorizing release of a decryption key; and

sending the decryption key for decryption of the encrypted content.

2. A method as recited in claim 1, wherein the confirmation is based on payment for the transmitted encrypted content.

3. A method as recited in claim 1, wherein the shared secret identifies a user, the device, or both.

4. A method as recited in claim 1, wherein the shared secret is a credit card number or a phone number.

5. A method as recited in claim 1, further comprising:

receiving from the device an acknowledgement indicating receipt of the decryption key.

6. A method as recited in claim 1, wherein the decryption key is sent to the device via the insecure communication channel.

7. A method as recited in claim 1, wherein the decryption key is sent in plaintext form to a point of sale terminal via the secure channel.

8. A method as recited in claim 1, further comprising:
receiving a random plaintext from the device.

9. A method as recited in claim 8, wherein the shared secret is encoded by a hash function of a combination of the shared secret and the random plaintext.

10. A method as recited in claim 8, further comprising:
encrypting the decryption key before sending it to the device.

11. A method as recited in claim 10, wherein the decryption key is encrypted using at least the shared secret and, optionally, the random plaintext secret.

12. A method as recited in claim 1, further comprising:
receiving from the device a content download confirmation value that is encoded with the shared secret.

13. A method as recited in claim 12, wherein the content download confirmation value is based on an MD5 checksum.

14. A method as recited in claim 12, wherein the content download confirmation value is based on a calculation using the shared secret.

15. A method as recited in claim 12, wherein the step of receiving confirmation further comprises:
receiving a random plaintext from the device;
receiving a hash of the shared secret and the random plaintext for each shared secret ;
computing a hash of the shared secret with the random plaintext to produce a cyphertext for each shared secret;
comparing the cyphertext to each of the received hash of each of the shared secrets; and
in the case of a match,

identifying the corresponding transmitted encoded content,

encoding a content download confirmation value for the transmitted encoded content using the shared secret; and

comparing the computed content download confirmation value to the received content download confirmation value to verify a complete content download.

16. A method as recited in claim 15, further comprising:

after verification of the complete content download, causing a prompt to be sent to a user of the device to purchase the downloaded content; and

receiving a confirmation of receipt of payment.

17. A method as recited in claim 1, wherein content stored in the content server is encrypted prior to a start of a download process.

18. A method for downloading content from a content server over an insecure communications channel, comprising:

sending a shared secret in an encoded form to a content server via an insecure communications channel;

downloading from the content server an encrypted content via the insecure channel;

sending an encoded content download confirmation value to the content server via the insecure communications channel;

receiving a decryption key in an encrypted form from the content server via the insecure communications channel, wherein the decryption key is encrypted using the shared secret;

decrypting the downloaded decryption key using the shared secret;

decrypting the downloaded encrypted content using the decryption key; and

sending an acknowledgement of the received decryption key.

19. The method of claim 18 further comprising:

providing an indicia of acceptance of terms of the download and decryption of the encrypted content by the user, wherein the indicia is an indication of acceptance of payment.

20. A method of authorizing a release of a decryption key corresponding to a downloaded content, comprising:

receiving from a user via a secure channel a shared secret in a plaintext form;

sending the shared secret to a content server;

receiving a confirmation of successful encrypted content download from the content server;

prompting the user to accept terms of download and decryption of the encrypted content; and

after receipt of an indicia of such acceptance, sending an authorization to the content server to release a decryption key for decrypting the downloaded encrypted content.

21. A system for transmitting a file to a device, comprising:

a content server operative to store a plurality of content files, to wirelessly transmit the content files via an insecure channel, and to communicate with via a secure channel;

one or more remote devices operative to transmit and receive communications to and from the content server over the insecure channel including anyone of the content files in encrypted form, each device including a processor to manage the communications as well as encryption and decryption of communicated data;

a point of sale terminal operative to communicate with a user associated with any of the devices; and

a payment server communicatively disposed between the point of sale terminal and the content server, and communicating therewith via the secure channel, further operative to provide a shared secret in plaintext form via the secured channel from the user to the content server, wherein the content server is further operative to release a decryption key to one of the devices upon receipt of confirmation from payment server that the user of the device accepted terms of download and decryption of a content file, wherein the decryption key is encrypted using the shared secret.

22. A computer readable program embodied on a computer readable medium for facilitating content download from a content server to a device via an insecure communications channel, comprising:

program code for causing a computer to receive a shared secret in an encoded form from a device, the encoded shared secret functioning as a device identifier;

program code for causing a computer to transmit content in an encrypted form from a content server to the device;

program code for causing a computer to receive the shared secret in plaintext form via a secure channel;

program code for causing a computer to receive a confirmation authorizing the release of a decryption key for the transmitted encrypted file; and

program code for causing a computer to send the decryption key for decrypting the transmitted encrypted file for which the payment confirmation has been received.

23. The computer program embodied on a computer readable medium of claim 22 wherein the confirmation is sent upon payment by a user of the device for the downloaded content.

24. A computer readable program embodied on a computer readable medium for downloading content from a content server, over an insecure communications channel, comprising:

code for sending a shared secret in an encoded form to a content server;

code for receiving from the content server an encrypted content;

code for sending an encoded content download confirmation value to the content server;

code for receiving an encrypted decryption key from the content server, wherein the decryption key is encrypted using the shared secret;

code for decrypting the encrypted decryption key using the shared secret;

code for decrypting the downloaded encrypted content using the decryption key; and

code for sending an acknowledgement of the received decryption key;

25. The computer readable program embodied on a computer readable medium of claim 24 further comprising:

code for providing an indicia of acceptance of terms of the download and decryption of the encrypted content by the user, wherein the indicia is an indication of acceptance of payment.

26. A computer readable program embodied on a computer readable medium for authorizing a release of a decryption key corresponding to a downloaded content, comprising:

code for receiving a shared secret in a plaintext form from a user, via a secure channel;

code for sending the shared secret to a content server;

code for receiving a confirmation of successful encrypted content download from the file server;

code for prompting the user to purchase the downloaded encrypted content; and

code for, after receipt of payment, sending an authorization to the content server to release a decryption key operative to decrypt the downloaded encrypted file.

27. A method of facilitating content download via an insecure communications channel, comprising:

receiving a concealed identifier from a device wherein the concealed identifier identifies the device;

transmitting an encrypted file to the device via an insecure channel, wherein the encrypted file has a corresponding decryption key;

receiving the identifier in an unconcealed form over a secure channel;

receiving an authorization from a payment server over the secure channel;

encrypting the key using the identifier; and

transmitting the encrypted key to the device.

28. A method for payment of file downloads to a wireless device, comprising:

receiving a concealed identifier from a device, wherein the identifier corresponds to the wireless device;

transferring a selected encrypted file to the wireless device, wherein the selected file is encrypted using a key;

receiving the identifier in an unconcealed form over a secure channel as part of a payment transaction;

using the identifier to encrypt the key; and

transmitting the encrypted key to the wireless device after receipt of payment.

29. A system for transmitting content via an insecure communications channel, comprising:

means for receiving a shared secret in an concealed form, from a device, wherein the shared secret identifies the device;

means for transferring a selected content in an encrypted form to the device, wherein the selected file has a corresponding decryption key;

means for receiving the shared secret in an unconcealed form over a secure channel as part of a payment transaction;

means for using the shared secret to encrypt a decryption key;

means for transmitting the encrypted decryption key to the wireless device after receipt of payment.

30. An apparatus for content download to a device via an insecure channel comprising:

means for receiving at least one identifier from a device, wherein the identifier is concealed and identifies the device;

means for transmitting an encrypted file to the device;

means for transmitting after receipt of an authorization, a decryption key encrypted using the identifier, wherein the decryption key can decrypt the encrypted file.